



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Digital Forensics Analysis (ACCA7031_LON)

Lecture 3

Cyber Forensics Investigative Process

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Content covered

- Secure digital evidence at an incident scene
- Catalog digital evidence
- Data Acquisition and Capturing the *Data Image*
- Store digital evidence, Obtain a digital hash
- Process and handle digital evidence
- Analysis and Investigative computer evidence (Windows, Linux and MacOS)

Objectives

- Understand how to Secure and Catalog digital evidence
- Understand Image capturing and data acquisition process and requirements
- Understand how image verify and integrity check works
- Examine chain of custody in DFIR context
- Aware of ACPO's Good Practice Guide for Computer-Based Electronic Evidence
- Understand the investigative process in context of computer evidence for different Operation Systems.

Securing Digital Evidence at an Incident Scene

- Depends on the nature of the case
- Guidelines:
 - Create a forensics copy
 - Still- and video-record the scene
 - Be invisible

Cataloging Digital Evidence

- If the digital evidence **is turned off**
 - Identify the type of computer or digital device
 - Photograph all cable connections
 - Label cables with evidence tags
 - Assign one person to collect and log evidence
 - Tagging
 - Current date and time
 - Serial numbers
 - Make and model
 - Maintain two separated logs for backup purposes
 - Maintain constant control of the evidence collected and the scene

Cataloging Digital Evidence (continued)

- If the digital evidence is **powered-on**
 - Photograph the screen contents first
 - Save active data to removable media
 - Copy any application data on screens
 - Save RAM data to removable media
 - Shutdown the computer
 - Use another OS to examine hard disk data
 - Create a bit-stream copy of the suspect's hard disk
 - Verify integrity of the forensic copy

Cataloging Digital Evidence (continued)



Understanding Bit-stream Copies

- Bit-by-bit copy of the original (evidence) storage medium
- Exact copy of the original disk
- Different from a simple backup copy
 - Backup software only copy known files
 - Backup software cannot copy deleted files or e-mail messages, or recover file fragments
- A bit-stream image file contains the bit-stream copy of all data on a disk or partition
- Preferable to copy the image file to a target disk that matches the original disk's manufacturer, size, and model

Understanding Bit-stream Copies (cont.)

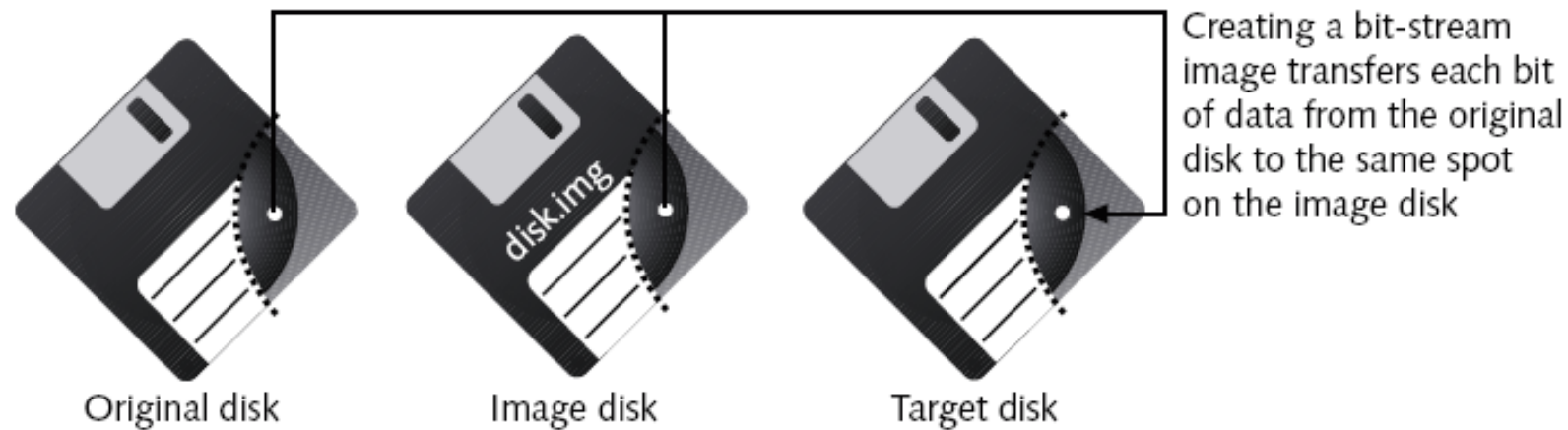
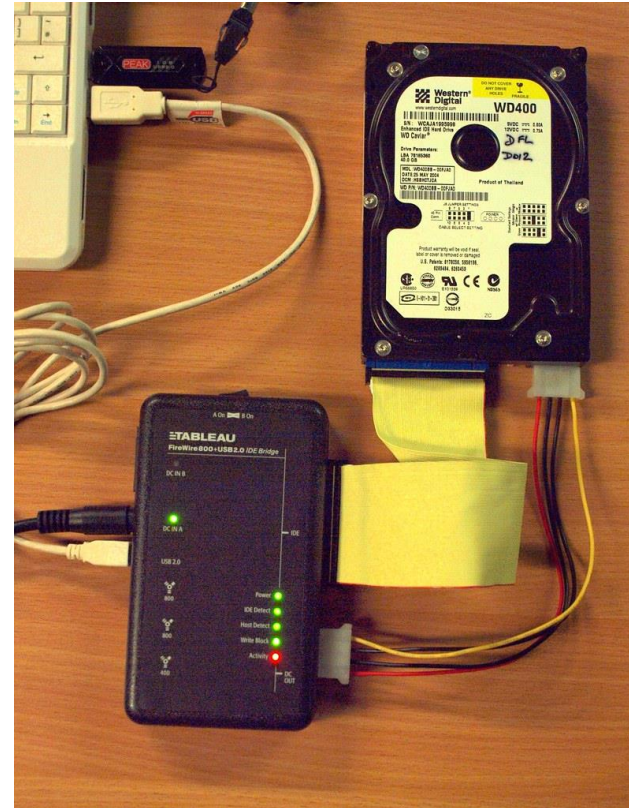


Figure 2-8 Transfer of data from original to bit-stream image to target

Hard Drive Imaging Example

https://live.staticflickr.com/6111/6285946610_e2372bd0b2_b.jpg



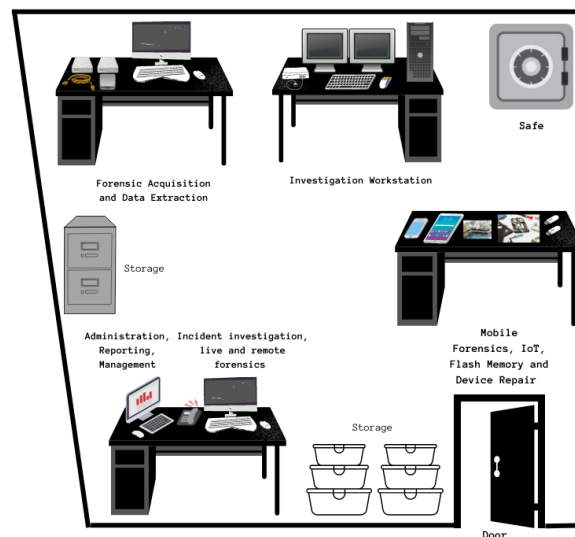
Lab Evidence Role

- Transport evidence to your lab
 - Ensure security and integrity of digital evidence
- Record your activities and findings
- Goal
 - Reproduce the same results
- Save your journal for future references
 - At court
 - Training

Digital Forensics Laboratory



Digital Forensics Lab



Digital Forensics Laboratory (cont.)



Processing and Handling Digital Evidence

- Create a bit-stream copy
 - Use a write-blocking device or embedded software
- Preserve the image file
- Steps:
 - Copy all bit-stream images to a large hard disk
 - Start forensics tools
 - Check bit-stream image file integrity
 - Place the original media in an evidence locker

Storing Digital Evidence

- Considerations:
 - How to save
 - What type of media
 - Where to store it
 - For how long
- Ideal media:
 - External HDD, Storage bay and **DVDs**
- Other storage options—magnetic tapes
 - 4mm DAT (4GB)
 - DLT (80GB)
 - Super-DLT or SDLT (RAIDs)
- Do not rely on only one method

Storing Digital Evidence (cont.)



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

<http://www.safeoptions.co.uk/master-lock-fire-safe-lfw123ftc>

Transforming Education: Transforming Lives
<https://www.synology.com/en-uk/products/DS420+>

Understanding Storage Formats for Digital Evidence

- Three formats
 - Raw format
 - Proprietary formats
 - Advanced Forensics Format (AFF)

Raw Format

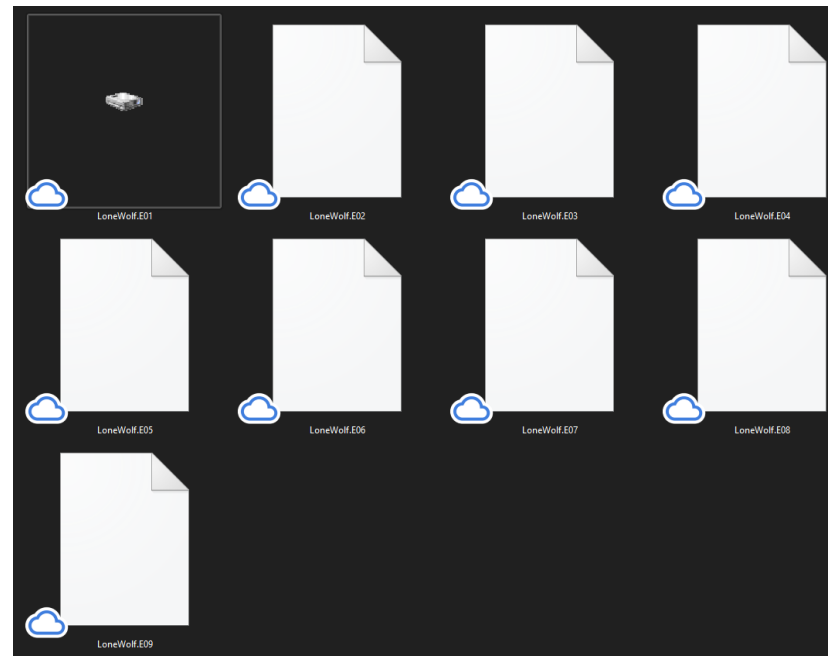
- Makes it possible to write bit-stream data to files
- Advantages
 - Fast data transfers
 - Can ignore minor data read errors on source drive
 - Most computer forensics tools can read raw format
- Disadvantages
 - Requires as much storage as original disk or data
 - Tools might not collect marginal (bad) sectors

Proprietary Formats

- Features offered
 - Option to compress or not compress image files
 - Can split an image into smaller segmented files
 - Can integrate metadata into the image file
- Disadvantages
 - Inability to share an image between different tools
 - File size limitation for each segmented volume

Proprietary Formats (cont.)

- One example would be the .E01 format used by FTK



Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
- Design goals
 - Provide compressed or uncompressed image files
 - No size restriction for disk-to-image files
 - Provide space in the image file or segmented files for metadata
 - Simple design with extensibility
 - Open source for multiple platforms and Oss.
 - Internal consistency checks for self-authentication
- File extensions include .afd for segmented image files and .afm for AFF metadata
- AFF is open source

Determining the Best Acquisition Method

- Types of acquisitions
 - Static acquisitions and live acquisitions
- Four methods
 - Bit-stream disk-to-image file
 - Bit-stream disk-to-disk
 - Logical disk-to-disk or disk-to-disk data
 - Sparse data copy of a file or folder

Determining the Best Acquisition Method (cont.)

- Bit-stream disk-to-image file
 - Most common method
 - Can make more than one copy
 - Copies are bit-for-bit replications of the original drive
 - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, XWays, iLook
- Bit-stream disk-to-disk
 - When disk-to-image copy is not possible
 - Consider disk's geometry configuration
 - EnCase, SafeBack, SnapCopy

Determining the Best Acquisition Method (cont.)

- Logical acquisition or sparse acquisition
 - When your time is limited
 - Logical acquisition captures only specific files of interest to the case
 - Sparse acquisition also collects fragments of unallocated (deleted) data
 - For large disks
 - PST or OST mail files, RAID servers

Determining the Best Acquisition Method (cont.)

- When making a copy, consider:
 - Size of the source disk
 - Lossless compression might be useful
 - Use digital signatures for verification
 - When working with large drives, an alternative is using tape backup systems
 - Whether you can retain the disk

Obtaining a Digital Hash

- Obtain a unique identity for file data
- Cyclic Redundancy Check (CRC)
 - One of the first methods
 - Most recent version CRC-32
- MD5
 - Most common algorithm
 - Mathematical formula translates a file into a hexadecimal value
- Secure Hash Algorithm (SHA)
 - Developed by NIST (128 bits known as SHA-1)

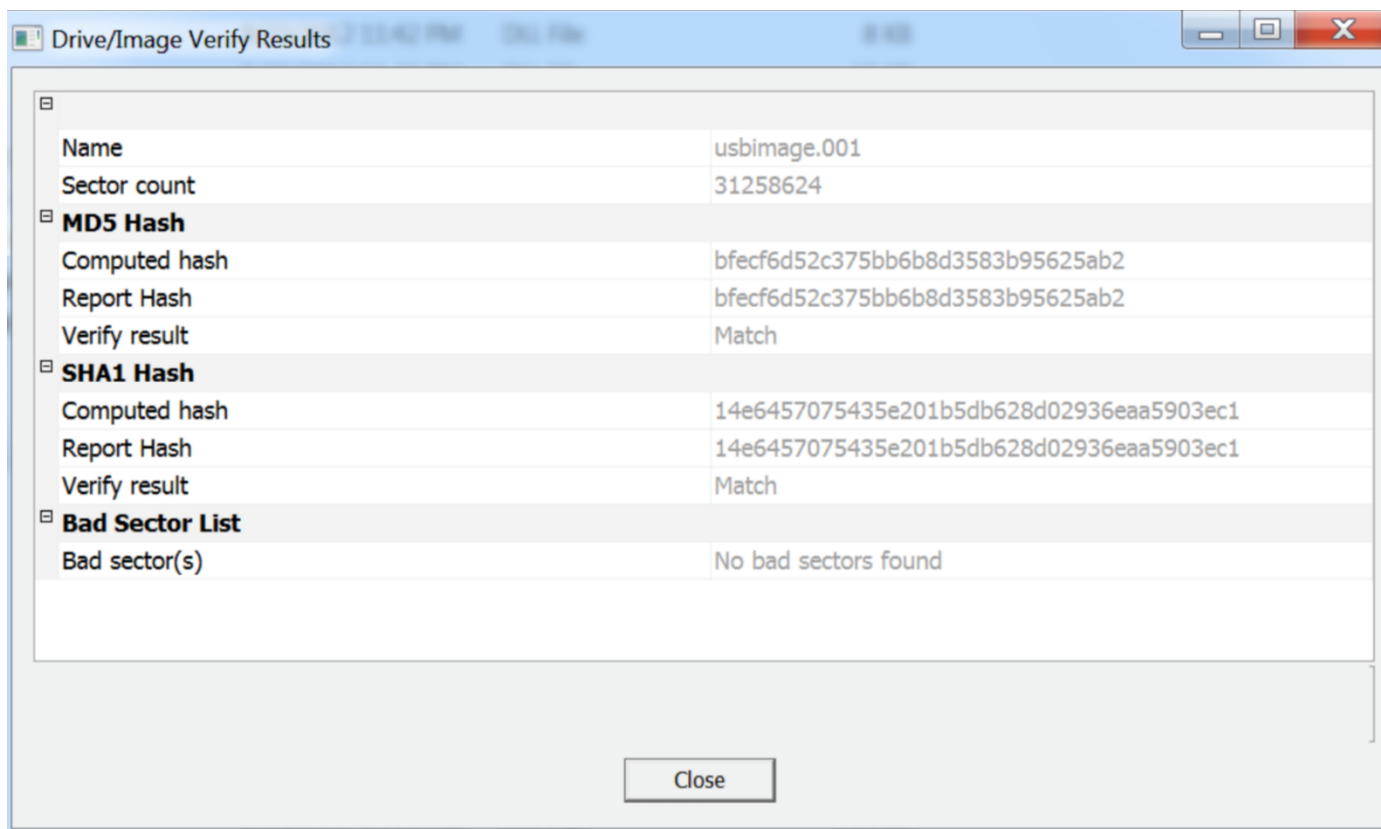
Obtaining a Digital Hash (cont.)

- Digital hash changes if a bit or byte changes
- Verification process
 - Create a hash value
 - Analyze data
 - Create a second hash value
 - Compare hash values

Obtaining a Digital Hash (cont.)

- Digital hashes are like digital fingerprints
- Non-keyed hash set can identify known programs
 - Unique hash number generated by a software tool
 - Identify known files (something hidden)
- Keyed hash set can produce a unique fingerprint
 - Generated by an encryption utility's secret key

Obtaining a Digital Hash (cont.)



Obtaining a Digital Hash (cont.)

- Example:
 - Create a file with Notepad
 - Obtain its hash value with EnCase/ FTK/ UFED/ XRY ...
 - Modify the file
 - Recompute its hash value
 - Compare hash values

ACPO's Good Practice Guide for Computer-Based Electronic Evidence

1. Personnel attending crime scenes or making initial contact with a victim/witness/suspect
2. Investigators
3. Evidence recovery staff
4. External consulting witnesses

ACPO's *Good Practice Guide for Computer-Based Electronic Evidence* (cont.)

- Personnel attending crime scenes or making initial contact with a victim/witness/suspect
 - securing, seizing and transporting equipment from search scenes with a view to recovering computer-based electronic evidence, as well as in the identification of the information needed to investigate a high-tech crime.
- Investigators
 - Planning and management by investigators of the identification, presentation and storage of computer-based electronic evidence.

ACPO's *Good Practice Guide for Computer-Based Electronic Evidence (cont.)*

- Evidence recovery staff

Recovery and reproduction of seized computer-based electronic evidence by personnel who are trained to carry out the function and have relevant training to give evidence in court of their actions. Persons who have not received the appropriate training and are unable to comply with the principles, must not carry out this category of activity.

- External consulting witnesses

The selection and management of persons who may be required to assist in the recovery, identification and interpretation of computer-based electronic evidence.

Four Principles Involved in Computer-based Electronic Evidence

- Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

- Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Four Principles Involved in Computer-based Electronic Evidence

- Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

- Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Operating Systems Forensics

- 3 key different operating systems commonly used:
 - Microsoft Windows
 - Mac OS
 - Linux

Microsoft Windows Forensics

- The file systems used by Windows include FAT, exFAT, NTFS, and ReFS. Investigators can search out evidence by analyzing the following important locations of the Windows:
 - Recycle Bin
 - Registry
 - Thumbs.db Files
 - Browser History
 - Print Spooling

Mac OS Forensics

- Mac OS X is the UNIX-based operating system that contains a Mach 3 microkernel and a FreeBSD-based subsystem.
- Mac OS X offers a novel technique to create a forensic duplicate. To do so, the perpetrator's computer should be placed into a "Target Disk Mode." Using this mode, the forensic examiner creates a forensic duplicate of perpetrator's hard disk with the help of a Firewire cable connection between the two PCs.

Linux Forensics

- Linux is an open source, Unix-like, and elegantly designed operating system.
- Unlike other OSs, Linux holds many file systems of the ext family, including ext2, ext3, and ext4. Linux can provide an empirical evidence if the Linux-embedded machine is recovered from a crime scene. In this case, forensic investigators should analyze the following folders and directories:
 - /etc [%SystemRoot%/System32/config]
 - /var/log
 - /home/\$USER
 - /etc/passwd

Modified Accessed Created (MAC)

- Last modified (or written) date
- Last accessed date
- File creation date
- Different types of file activities set or update the different date stamps
- Key to reporting and proving evidence

Summary

1. Evidence acquisition and preservation from Incident Scene
2. Forensics imaging mode and formats
3. Hashing, Acquisition validation and Integrity check
4. Investigating Windows, Linux and MacOS machines
5. Data reconstruction and examination
6. Modification, Access and Creation time



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk